I CLAIM:

1. A computer program product comprising a computer program operable to control a reporting computer to report occurrence of an event to a receiving computer, said computer program comprising:

report generating logic operable to generate report data identifying said reporting computer and said event;

data retrieving logic operable to fetch requested data from said receiving computer to said reporting computer upon a request of said reporting computer; and

report sending logic operable to send said report data from said reporting computer to said receiving computer upon fetching of said requested data.

2. A computer program product as claimed in claim 1, wherein said event is detection of a computer file containing an unwanted computer program.

3. A computer program product as claimed in claim 2, wherein said unwanted computer program is a computer virus.

4. A computer program product as claimed in claim 1, wherein said requested data is a description of said event.

5. A computer program product as claimed in claim 1, wherein said event is detection of a computer file containing a computer virus and said requested data is a description of said computer virus.

6. A computer program product as claimed in claim 1, wherein said event is detection of a computer file containing a computer virus and said requested data is an updated set of computer virus detecting data for use in detecting computer viruses.

7. A computer program product as claimed in claim 1, wherein said data retrieving logic and said report sending logic use an internet URL to specify said requested data to said receiving computer, said internet URL also containing said report data to be sent to said receiving computer.

8. A computer program product as claimed in claim 1, wherein said reporting computer collates report data specifying one or more events that is send together from said reporting computer to said receiving computer upon fetching of said requested data.

9. A computer program product as claimed in claim 1, wherein said report data is encrypted by said reporting computer and decrypted by said receiving computer.

10. A computer program product as claimed in claim 1, wherein said reporting computer and said receiving computer communicate via an internet link.

11. A computer program product as claimed in claim 1, wherein said report data includes one or more of:

a MAC address identifying a network card of said reporting computer;

a date of said event;

a time of said event;

an identifier of a computer program used by said reporting computer to detect said event;

an identifier of a version of a computer program used by said reporting computer to detect said event;

an identifier of a set of event detecting data used by a computer program used by said reporting computer to detect said event;

an identifier of an event type detected by said reporting computer;

an action taken by said reporting computer upon detection of said event; and

a checksum of a file that triggered said event.

12. A computer program product comprising a computer program operable to control a receiving computer to receive a report of occurrence of an event from a reporting computer, said computer program comprising:

data request receiving logic operable to receive a request for requested data from said reporting computer;

data providing logic operable to provide said requested data to said reporting computer; and

report receiving logic operable to receive report data identifying said reporting computer and said event from said reporting computer upon providing of said requested data to said reporting computer.

13. A computer program product as claimed in claim 12, wherein said event is detection of a computer file containing an unwanted computer program.

14. A computer program product as claimed in claim 13, wherein said unwanted computer program is a computer virus.

15. A computer program product as claimed in claim 12, wherein said requested data is a description of said event.

16. A computer program product as claimed in claim 12, wherein said event is detection of a computer file containing a computer virus and said requested data is a description of said computer virus.

17. A computer program product as claimed in claim 12, wherein said event is detection of a computer file containing a computer virus and said requested data is an updated set of computer virus detecting data for use in detecting computer viruses.

18. A computer program product as claimed in claim 12, wherein said request uses an internet URL to specify said requested data to said receiving computer, said internet URL also containing said report data to be sent to said receiving computer.

19. A computer program product as claimed in claim 12, wherein said report data specifies one or more events and is send together from said reporting computer to said receiving computer upon providing of said requested data.

20. A computer program product as claimed in claim 12, wherein said report data is encrypted by said reporting computer and decrypted by said receiving computer.

21. A computer program product as claimed in claim 12, wherein said reporting computer and said receiving computer communicate via an internet link.

22. A computer program product as claimed in claim 12, wherein said report data includes one or more of:

a MAC address identifying a network card of said reporting computer;

a date of said event;

a time of said event;

an identifier of a computer program used by said reporting computer to detect said event;

an identifier of a version of a computer program used by said reporting computer to detect said event;

an identifier of a set of event detecting data used by a computer program used by said reporting computer to detect said event;

an identifier of an event type detected by said reporting computer; and

an action taken by said reporting computer upon detection of said event; and

a checksum of a file that triggered said event.

23. A method of controlling a reporting computer to report occurrence of an event to a receiving computer, said method comprising the steps of:

generating report data identifying said reporting computer and said event;

fetching requested data from said receiving computer to said reporting computer upon a request of said reporting computer; and

sending said report data from said reporting computer to said receiving computer upon fetching of said requested data.

24. A method as claimed in claim 23, wherein said event is detection of a computer file containing an unwanted computer program.

25. A method as claimed in claim 24, wherein said unwanted computer program is a computer virus.

26. A method as claimed in claim 23, wherein said requested data is a description of said event.

27. A method as claimed in claim 23, wherein said event is detection of a computer file containing a computer virus and said requested data is a description of said computer virus.

28. A method as claimed in claim 23, wherein said event is detection of a computer file containing a computer virus and said requested data is an updated set of computer virus detecting data for use in detecting computer viruses.

29. A method as claimed in claim 23, wherein said data retrieving logic and said report sending logic use an internet URL to specify said requested data to said receiving computer, said internet URL also containing said report data to be sent to said receiving computer.

30. A method as claimed in claim 23, wherein said reporting computer collates report data specifying one or more events that is send together from said reporting computer to said receiving computer upon fetching of said requested data.

31. A method as claimed in claim 23, wherein said report data is encrypted by said reporting computer and decrypted by said receiving computer.

32. A method as claimed in claim 23, wherein said reporting computer and said receiving computer communicate via an internet link.

33. A method as claimed in claim 23, wherein said report data includes one or more of:

a MAC address identifying a network card of said reporting computer;

a date of said event;

a time of said event;

an identifier of a computer program used by said reporting computer to detect said event;

an identifier of a version of a computer program used by said reporting computer to detect said event;

an identifier of a set of event detecting data used by a computer program used by said reporting computer to detect said event;

an identifier of an event type detected by said reporting computer;

an action taken by said reporting computer upon detection of said event; and

a checksum of a file that triggered said event.

34. A method of controlling a receiving computer to receive a report of occurrence of an event from a reporting computer, said method comprising the steps of:

receiving a request for requested data from said reporting computer;

providing said requested data to said reporting computer; and

receiving report data identifying said reporting computer and said event from said reporting computer upon providing of said requested data to said reporting computer.

35. A method as claimed in claim 34, wherein said event is detection of a computer file containing an unwanted computer program.

36. A method as claimed in claim 35, wherein said unwanted computer program is a computer virus.

37. A method as claimed in claim 34, wherein said requested data is a description of said event.

38. A method as claimed in claim 34, wherein said event is detection of a computer file containing a computer virus and said requested data is a description of said computer virus.

39. A method as claimed in claim 34, wherein said event is detection of a computer file containing a computer virus and said requested data is an updated set of computer virus detecting data for use in detecting computer viruses.

40. A method as claimed in claim 34, wherein said request uses an internet URL to specify said requested data to said receiving computer, said internet URL also containing said report data to be sent to said receiving computer.

41. A method as claimed in claim 34, wherein said report data specifies one or more events and is send together from said reporting computer to said receiving computer upon providing of said requested data.

42. A method as claimed in claim 34, wherein said report data is encrypted by said reporting computer and decrypted by said receiving computer.

43. A method as claimed in claim 34, wherein said reporting computer and said receiving computer communicate via an internet link.

44. A method as claimed in claim 34, wherein said report data includes one or more of:

a MAC address identifying a network card of said reporting computer;

a date of said event;

a time of said event;

an identifier of a computer program used by said reporting computer to detect said event;

an identifier of a version of a computer program used by said reporting computer to detect said event;

an identifier of a set of event detecting data used by a computer program used by said reporting computer to detect said event;

an identifier of an event type detected by said reporting computer; and

an action taken by said reporting computer upon detection of said event; and

a checksum of a file that triggered said event.

45. A reporting computer operable to report occurrence of an event to a receiving computer, said reporting computer comprising:

a report generator operable to generate report data identifying said reporting computer and said event;

a data retriever operable to fetch requested data from said receiving computer to said reporting computer upon a request of said reporting computer; and

a report sender operable to send said report data from said reporting computer to said receiving computer upon fetching of said requested data.

46. A reporting computer as claimed in claim 45, wherein said event is detection of a computer file containing an unwanted computer program.

47. A reporting computer as claimed in claim 46, wherein said unwanted computer program is a computer virus.

48. A reporting computer as claimed in claim 45, wherein said requested data is a description of said event.

49. A reporting computer as claimed in claim 45, wherein said event is detection of a computer file containing a computer virus and said requested data is a description of said computer virus.

50. A reporting computer as claimed in claim 45, wherein said event is detection of a computer file containing a computer virus and said requested data is an updated set of computer virus detecting data for use in detecting computer viruses.

51. A reporting computer as claimed in claim 45, wherein said data retrieving logic and said report sending logic use an internet URL to specify said requested data to said receiving computer, said internet URL also containing said report data to be sent to said receiving computer.

52. A reporting computer as claimed in claim 45, wherein said reporting computer collates report data specifying one or more events that is send together from said reporting computer to said receiving computer upon fetching of said requested data.

53. A reporting computer as claimed in claim 45, wherein said report data is encrypted by said reporting computer and decrypted by said receiving computer.

54. A reporting computer as claimed in claim 45, wherein said reporting computer and said receiving computer communicate via an internet link.

55. A reporting computer as claimed in claim 45, wherein said report data includes one or more of:

a MAC address identifying a network card of said reporting computer;

a date of said event;

a time of said event;

an identifier of a computer program used by said reporting computer to detect said event;

an identifier of a version of a computer program used by said reporting computer to detect said event;

an identifier of a set of event detecting data used by a computer program used by said reporting computer to detect said event;

an identifier of an event type detected by said reporting computer;

an action taken by said reporting computer upon detection of said event; and

a checksum of a file that triggered said event.

56. A receiving computer operable to receive a report of occurrence of an event from a reporting computer, said receiving computer comprising:

a data request receiver operable to receive a request for requested data from said reporting computer;

a data provider operable to provide said requested data to said reporting computer; and

a report receiver operable to receive report data identifying said reporting computer and said event from said reporting computer upon providing of said requested data to said reporting computer.

57. A receiving computer as claimed in claim 56, wherein said event is detection of a computer file containing an unwanted computer program.

58. A receiving computer as claimed in claim 57, wherein said unwanted computer program is a computer virus.

59. A receiving computer as claimed in claim 56, wherein said requested data is a description of said event.

60. A receiving computer as claimed in claim 56, wherein said event is detection of a computer file containing a computer virus and said requested data is a description of said computer virus.

61. A receiving computer as claimed in claim 56, wherein said event is detection of a computer file containing a computer virus and said requested data is an updated set of computer virus detecting data for use in detecting computer viruses.

62. A receiving computer as claimed in claim 56, wherein said request uses an internet URL to specify said requested data to said receiving computer, said internet URL also containing said report data to be sent to said receiving computer.

63. A receiving computer as claimed in claim 56, wherein said report data specifies one or more events and is send together from said reporting computer to said receiving computer upon providing of said requested data.

64. A receiving computer as claimed in claim 56, wherein said report data is encrypted by said reporting computer and decrypted by said receiving computer.

65. A receiving computer as claimed in claim 56, wherein said reporting computer and said receiving computer communicate via an internet link.

66. A receiving computer as claimed in claim 56, wherein said report data includes one or more of:

a MAC address identifying a network card of said reporting computer;

a date of said event;

a time of said event;

an identifier of a computer program used by said reporting computer to detect said event;

an identifier of a version of a computer program used by said reporting computer to detect said event;

an identifier of a set of event detecting data used by a computer program used by said reporting computer to detect said event;

an identifier of an event type detected by said reporting computer; and

an action taken by said reporting computer upon detection of said event; and

a checksum of a file that triggered said event.